UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,718	04/16/2004	Glen Anderson	P2007US00	2184

24333 7590 04/30/2008

GATEWAY, INC.
ATTN: Patent Attorney
610 GATEWAY DRIVE
MAIL DROP Y-04
N. SIOUX CITY, SD 57049

EXAMINER	
NGUYEN, PHILLIP H	
ART UNIT	**PAPER NUMBER**
2191	

MAIL DATE	DELIVERY MODE
04/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/826,718	ANDERSON, GLEN	
	Examiner	Art Unit	
	Phillip H. Nguyen	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,19-37,39-48 and 50-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,19-37,39-48 and 50-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed 2/06/2008.

2. Per applicant's request, claims 1, 35, 42, 46-48, 50, and 51 have been amended; claims 18, 38, and 49 have been cancelled.

3. Claims 1-17, 19-37, 39-48, and 50-53 remain pending and have been considered below.

Response to Arguments

4. Applicant's arguments with respect to claims 1-53 have been considered but are moot in view of the new ground(s) of rejection.

Examiner's Note

5. Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in claim 42 by using "means-plus-function" language. However, examiner notes that the only "means" for performing these cited functions in the specification appears to be software. Since no other specific structural limitations are disclosed in the specification, the claim has not invoked 35 U.S.C. 112 6th paragraph when considered below.

Claim Objections

6. Claims 5, 8-10, 12, 35, 37, and 46 are objected to because of the following informalities: The claims recite the phrases “adapted to” or "configured to" in the body of the claim. It indicates intended use and as such do not carry any patentable weight.

Limitations following the phrase “adapted to” or “configured to” describe intended use but not necessarily required functionality of the claim. Applicant is suggested to amend the claims so that the limitations are recited in a definite format. For example, changing "adapted to initiate" to "initiates" or “configure to execute" to “executes”.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 2, 4, 7, 8, 10, 11, 15-17, 19, 20, 22-24, 26-30, 33, 35-37, 41, 46, 50, and 52 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas Jr. et al. (USPN 7,051,211).

As per claim 1:

Matyas Jr. teaches:

associating, by said download manager, a transaction identifier with selection data comprising a software selection (see at least col. 9:38-53 “*The target data processing system 106 and/or 106' also starts the execution of the*

unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by sending the information, along with the ***product ID value*** *to the software installation server 102*"), said selection data being determined at the time of sale of the hardware unit (see at least col. 9:21-24 "*with each instance of* ***sold software*** *there may also* ***be associated a secret value A***");

sending a download transaction request comprising the transaction identifier from the download manager to the download supervisor (see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***"); and

responsive to determining, by the download supervisor, that the requested download transaction is authorized (see at least col. 10:6-9 "*When the software installation server 102 receives the message over the network 104, it will try to identify the instance of the product and* ***verify that the user is the legitimate customer***"), *performing the steps of:*

assembling, by the download supervisor, a download/installation instruction comprising up-to-date software access information for the software selection (see at least col. 10:20-22 "*Upon sending A, the*

software installation server 102 may assign a new value, A_new, in the software installation repository 100 to correspond to the (ID, S) pair");

communicating the download/installation instruction from the download supervisor to the download manager (see at least col. 10:14-15 "*send the secret value A in the clear to the target data processing system 106 and/or 106*"); and

performing, by the download manager, a download and installation of the software selection to the hardware unit pursuant to the download/installation instruction (see at least col. 10:37-43 "*The decrypted* ***software P may be installed on the target data processing system 106 and/or 106'*** *by the unencrypted portion of the software. Software P will be re-encrypted with the new key K_new-Hash (S,K) and* ***stored on a writable storage media at the target data processing system 106 and/or 106"***).

As per claim 2:

Matyas Jr. further teaches:

wherein the transaction identifier comprises a serial number (see at least col. 8:50-51 "***product identification information (ID)****, S value and A values* ***associated with particular copies of the software*** *to be controlled*").

As per claim 4:

Matyas Jr. further teaches:

wherein the first software handling machine comprises the hardware unit (see at least FIGS. 2-3).

As per claim 7:

Matyas Jr. further teaches:

wherein the first software handling machine comprises a personal computer (see at least FIGS. 2-3; see also col. 11:62-63 "*Such data processing system may include for example,* ***personal computers, laptop computers***...").

As per claims 8 and 37:

Matyas Jr. further teaches:

wherein the download manager is configured to launch from the hardware unit (see at least col. 9:34-40 "*when the user loads the received software code into the target data processing system 106 and/or 106', the target data processing system 106 and/or 106' makes a connection through the network 104, for example, through the Internet, to the software installation server 102. The target data processing system 106 and/or 106' also* ***start the execution of the unencrypted portion of the software located in the code***").

As per claims 10 and 17:

Matyas Jr. further teaches:

wherein the download manager is preconfigured to send a download transaction request comprising a predetermined selection of software (see at least col. 9:51-53 "*requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***").

As per claim 11:

Matyas Jr. further teaches:

wherein the hardware unit is linked to the first software handling machine by a dedicated communications link (see at least FIG. 3; see also col. 12:7-8 "*The processor 238 communicates with the memory 236 via an* ***address/data bus*** *248*").

As per claims 15, 29, and 50:

Matyas Jr. further teaches:

storing a record of the download transaction in a central database (see at least col. 8:50-52 "*the* ***software installation repository 100 may contain product identification information (ID)****, S values and A values associated with particular copies of the software to be controlled*").

As per claim 16:

Matyas Jr. further teaches:

wherein data comprising the transaction identifier is encrypted (see at least col. 8:38-40 "*The values S and A are utilized to derive the encryption key "K" which may be used to decrypted the encrypted portion of the software*").

As per claim 19:

Matyas Jr. further teaches:

wherein the selection data is determined in whole or in part in an interactive process (see at least col. 9:51-53 "*requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***").

As per claim 20:

Matyas Jr. further teaches:

obtaining the selection data by a point of sale application (see at least col. 9:22-24 "*with each instance of sold software there may also be associated a secret value A*").

As per claim 22:

Matyas Jr. further teaches:

wherein the selection data is determined in whole or in part by looking up the transaction identifier in a central database (see at least col. 10:9-12 "*As described above, the (ID, S) pair has a corresponding value A in the software installation repository 100 which the* ***software installation server 102 may access to authorized the installation***").

As per claim 23:

Matyas Jr. further teaches:

wherein determining whether the download transaction is authorized comprises evaluating the transaction identifier (see at least col. 10:9-12 "*As described above, the* ***(ID, S) pair has a corresponding value A*** *in the software installation repository 100 which the* ***software installation server 102 may access to authorized the installation***").

As per claim 24:

Matyas further teaches:

interrogating the hardware unit to obtain information comprising preexisting software (see at least col. 9:54-57 "*the unencrypted portion of the software might also determine the unique identifier of the target data processing system 106 and/or 106' or other such parameters and send these further parameters to the software installation server 102*").

As per claim 26:

Matyas Jr. further teaches:

modifying the selection data in response to the information comprising preexisting software (see at least col. 14:62-67 – col.15:1-8 "*the user's client computer may read the software code from the medium on which it is received and store it on a second medium, where the user's client computer has a capability to read and write information on that second medium (e.g., a file stored on a hard disk). If the software code is received on a medium such that the user's client computer can read and write information to that medium, then the user's client computer may have the option to leave the software code on the received medium or alternatively read software code form the medium and store it on the second read-write medium…*").

As per claims 27 and 36:

Matyas Jr. further teaches:

wherein the software access information comprises an authentication code for activating or downloading software (see at least col. 10:9-12 "*As described above, the* ***(ID, S) pair has a corresponding value A*** *in the software installation repository 100 which the* ***software installation server 102 may access to authorized the installation***").

As per claim 28:

Matyas Jr. further teaches:

wherein the authentication code is provided by an authentication subsystem of the download supervisor (see at least col. 9:51-53 "*request authorization to install the software by sending the information, along with the product ID value to the software installation server 102*").

As per claim 30:

Matyas Jr. further teaches:

wherein the download transaction data comprises a download transaction status (see at least col. 16:20-30 "*if the user knows that this software can be installed 10 times, the software could be installed 9 times and then the user claim that there was a crash, obtain the original A value and then install the software 9 more times, and so on. To combat this attack the installation server may maintain the following values: A_original, A_current, M, N, M_max and N_max, where M_max is the number of times the original A value can be sent, M is the number of times it has been sent, N_max is the number of installations allowed and N is the number installation so far M_max, N_max should be greater than 0*").

As per claims 33, 41, and 52:

Matyas Jr. further teaches:

wherein the software is data comprising data related to services (*the software must be related to services in order to fulfill the purpose of software distribution from the vendor to clients*).

As per claim 35:

Matyas Jr. further teaches:

a plurality of software vendor download servers in the network for downloading software from the plurality of software vendors (see at least col. 9:26-29 "*The software installation server 102, operated on behalf of the software provider, may access the software installation repository 100 and, thereby, may possess the knowledge of every unit of software that was generated (and possibly sold)*");

a first software handling machine in the network and linked to the hardware unit, the first software handling machine configured to execute a download manager, the download manager adapted to initiate a download/installation transaction comprising selected software to be downloaded to the hardware unit from one or more of the plurality of software vendor download servers, to send a transaction identifier in a download transaction request to a download supervisor over the network (see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests*

authorization to install the software by ***sending*** *the information, along with* ***the product ID value to the software installation server 102***"), and to download and install the selected software to the hardware unit pursuant to a download/installation instruction received in response to the download transaction request, said selected software being determined at the time of sale of the hardware unit (see at least col. 10:37-43 "*The decrypted* ***software P may be installed on the target data processing system 106 and/or 106'*** *by the unencrypted portion of the software. Software P will be re-encrypted with the new key K_new-Hash (S,K) and* ***stored on a writable storage media at the target data processing system 106 and/or 106"***"); and

a second software handling machine in the network configured to execute the download supervisor, the download supervisor adapted to determine whether the download transaction request is authorized (see at least col. 10:6-9 "*When the software installation server 102 receives the message over the network 104, it will try to identify the instance of the product and* ***verify that the user is the legitimate customer***"), and, in response to determining that the transaction is authorized, to assemble a download/installation instruction comprising up-to-date software access information for the software selection and to send the download/installation instruction to the download manager (see at least col. 10:14-15 "*send the secret value A in the clear to the target data processing system 106 and/or 106"*");

wherein the first software handling machine is linkable to the hardware unit by an external bus, and wherein the download manager executes upon detecting that the hardware unit is linked to the first software handling machine by said external bus (see at least FIG. 3; see also col. 12:7-8 "*The processor 238 communicates with the memory 236 via an* ***address/data bus*** *248*").

As per claim 46:

Matyas Jr. further teaches:

provide a download manager executable on a first software handling machine in the network, the download manager being adapted to initiate a download/installation transaction comprising selected software to be downloaded to the hardware unit from one or more of said plurality of software vendor download servers in the network (see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***"), to provide a transaction identifier to a download supervisor to identify and validate the download transaction (see at least col. 10:6-9 "*When the software installation server 102 receives the message over the network 104, it will try to identify the instance of the product and* ***verify that the user is the legitimate customer***") and to

perform a download and an installation of selected software to the hardware unit pursuant to a download/installation instruction received from the download supervisor (see at least col. 10:37-43 "*The decrypted* ***software P may be installed on the target data processing system 106 and/or 106'*** *by the unencrypted portion of the software. Software P will be re-encrypted with the new key K_new-Hash (S,K) and* ***stored on a writable storage media at the target data processing system 106 and/or 106"***);

provide the download supervisor executable on a second software handling machine in the network, the download supervisor being adapted to receive the transaction identifier from the download manager, evaluate the transaction identifier to determine whether the download transaction is authorized and, in response to determining that the transaction is authorized, to communicate a download/installation instruction comprising up-to-date software access information for the selected software from the download supervisor to the download manager (see at least col. 10:6-9 "*When the software installation server 102 receives the message over the network 104, it will try to identify the instance of the product and* ***verify that the user is the legitimate customer***");

cause the download manager to be preconfigured for downloading a predetermined software selection determined at the time of sale of the hardware unit (see at least col. 9:34-40 "*When the user loads the received software code into the target data processing system 106 and/or 106',* ***the target data processing system 106 and/or 106' makes a connection through the***

network 104, for example, through the Internet, to the software installation server 102*. The target data processing system 106 and/or 106' also start the execution of the unencrypted portion of the software located in the code*");

associate the transaction identifier with the selected software for a download transaction(see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by sending the information, along with the* ***product ID value*** *to the software installation server 102*"), said selection data being determined at the time of sale of the hardware unit (see at least col. 9:21-24 "*with each instance of* ***sold software*** *there may also* ***be associated a secret value A***");

send a download transaction request comprising the transaction identifier over the network from the download manager to the download supervisor (see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***"); and

perform the download and installation of software to the hardware unit by the download manager pursuant to the download/installation instruction (see at least col. 10:37-43 "*The decrypted* ***software P may be installed on the target***

data processing system 106 and/or 106' *by the unencrypted portion of the software. Software P will be re-encrypted with the new key K_new-Hash (S,K) and* ***stored on a writable storage media at the target data processing system 106 and/or 106"***).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 3, 5, 6, 9, 39, 42-45, 47, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (USPN 7,051,211), in view of DaCosta et al. (USPAPN 2002/0120725).

<u>As per claims 3 and 39:</u>

Matyas Jr. does not explicitly teach:

wherein the software access information comprises a network address for a download server.

However, DaCosta teaches:

wherein the software access information comprises a network address for a download server (see at least [0010] "***the address information (e.g., a Web sit address)*** *is provided each time the application is booted up or updated*").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas's approach to include the teaching of DaCosta. One would have been motivated to modify because *the updates can be automatically retrieved each time the computer system is booted up or used, the updates can be distributed in a timely manner without inconveniencing the user. Significantly, applications can be automatically updated without having to execute the applications and transparent to the user, so that the user is not diverted from completing the task at hand* (see at least [0016]).

As per claims 5, 9, 47, and 48:

Matyas Jr. does not explicitly teach:

wherein the download manager is configured to **execute in a boot sequence** of the first software handling machine.

However, DaCosta teaches:

wherein the download manager is configured to execute in a boot sequence of the first software handling machine (see at least [0030] "*Agent 205 is a software program or set of computer-readable program instructions that implements the present invention method for updating applications. In one embodiment,* ***agent 205 is the boot loader that executes during boot up of computer system 190*** *(the boot loader runs at startup to initialize and configure system hardware)*").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas's approach to include the teach of DaCosta. One would have been motivated to modify because *the updates can be automatically retrieved each time the computer system is booted up or used, the updates can be distributed in a timely manner without inconveniencing the user. Significantly, applications can be automatically updated without having to execute the applications and transparent to the user, so that the user is not diverted from completing the task at hand* (see at least [0016]).

As per claim 6:

Matyas Jr. in combination with DaCosta teaches all the limitations of the base claim, Matyas further teaches:

> wherein the download manager loads from a removable storage media (see at least col. 14:53-58 "*In certain embodiment of the present invention, the software code may be received on a read-only storage medium. For example, the software code could be received on a Compact Disk (CD) and the user's client computer may have only a capability to read information stored on the CD but not write information on the CD*").

As per claim 42:

Matyas Jr. further teaches:

means to provide a transaction identifier and software selection data to a download supervisor in the network to enable the download supervisor to identify and validate the download transaction (see at least col. 9:38-53 "*The target data processing system 106 and/or 106' also starts the execution of the unencrypted portion of the software located in the code...The unencrypted portion of the software accepts the information provided by the user and requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***");

means to receive a communication from the download supervisor comprising a download/installation instruction that includes up-to-date software access information for the selected software of the download transaction, said software selection data being determined at the time of sale of the hardware unit (see at least col. 10:14-15 "*send the secret value A in the clear to the target data processing system 106 and/or 106*"); and

means to perform the download and installation of the selected software to the hardware unit according to the download/installation instruction (see at least col. 10:37-43 "*The decrypted* ***software P may be installed on the target data processing system 106 and/or 106'*** *by the unencrypted portion of the software. Software P will be re-encrypted with the new key K_new-Hash (S,K) and* ***stored on a writable storage media at the target data processing system 106 and/or 106"***).

Matyas Jr. does not explicitly teach:

means to initiate the download manager during a boot sequence of the hardware unit.

However, DaCosta teaches:

means to initiate the download manager during a boot sequence of the hardware unit (see at least [0030] "*Agent 205 is a software program or set of computer-readable program instructions that implements the present invention method for updating applications. In one embodiment,* ***agent 205 is the boot loader that executes during boot up of computer system 190*** *(the boot loader runs at startup to initialize and configure system hardware)*").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas's approach to include the teach of DaCosta. One would have been motivated to modify because *the updates can be automatically retrieved each time the computer system is booted up or used, the updates can be distributed in a timely manner without inconveniencing the user. Significantly, applications can be automatically updated without having to execute the applications and transparent to the user, so that the user is not diverted from completing the task at hand* (see at least [0016]).

As per claim 43:

Matyas Jr. in combination with DaCosta teaches all the limitations of the base claim, DaCosta further teaches:

wherein the means to initiate the download manager during a boot sequence of the hardware unit comprises executing a bootstrap loader to establish basic connectivity and download functions for the hardware unit in order to load a program to which the bootstrap loader hand off control (see at least [0030] "*Agent 205 is a software program or set of computer-readable program instructions that implements the present invention method for updating applications. In one embodiment,* ***agent 205 is the boot loader that executes during boot up of computer system 190 (the boot loader runs at startup to initialize and configure system hardware)***").

As per claim 44:

Matyas Jr. in combination with DaCosta teaches all the limitations of the base claim, Matyas Jr. further teaches:

wherein the selected software may be selected or modified by a user in an interactive process (see at least col. 14:62-67 – col.15:1-8 "*the user's client computer may read the software code from the medium on which it is received and store it on a second medium, where the user's client computer has a capability to read and write information on that second medium (e.g., a file stored on a hard disk). If the software code is received on a medium such that the user's client computer can read and write information to that medium, then the user's client computer may have the option to leave the software code on the*

received medium or alternatively read software code form the medium and store it on the second read-write medium…").

As per claim 45:

Matyas Jr. further teaches:

wherein the selected software comprises a predetermined selection (see at least col. 9:51-53 "*requests authorization to install the software by* ***sending*** *the information, along with* ***the product ID value to the software installation server 102***").

11. Claims 12-14, 21, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (USPN 7,051,211), in view of Gulliver et al. (USPAN 2004/0054597).

As per claim 12:

Matyas Jr. does not explicitly teach:

wherein the download manager is configured to execute upon detecting that the hardware unit is linked to the first software handling machine by the dedicated communication communications link.

However, Gulliver teaches:

wherein the download manager is configured to execute upon detecting that the hardware unit is linked to the first software handling machine by the

dedicated communication communications link (see at least [0023] "*The utility itself can be in the form of an applet that is* ***automatically launched when the PDA 26 is booted up***").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas Jr.'s approach to include the teaching of Gulliver. One would have been motivated to modify because it provides an automatically downloading without user interaction.

As per claim 13:

Matyas Jr. in combination with Gulliver teaches all the limitations of the base claim, Matyas Jr. further teaches:

wherein the hardware unit is linked to the first software handling machine over a network comprising a local area network (see at least col. 8:61-67 "*The network 104 may be an* ***intranet****, an extranet,* ***a virtual private network****, the internet*").

As per claim 14:

Matyas Jr. in combination with Gulliver teaches all the limitations of the base claim, Matyas Jr. further teaches:

wherein the network comprises the Internet (see at least col. 8:61-67 "*The network 104 may be an intranet, an extranet, a virtual private network, the* ***internet***").

As per claims 21 and 53:

Matyas Jr. does not explicitly teach:

wherein obtaining the selection data by a point of sale application comprises providing an automated kiosk for selecting software and recording the selections for a download transaction.

However, Gulliver teaches:

wherein obtaining the selection data by a point of sale application comprises providing an automated kiosk for selecting software and recording the selections for a download transaction (see at least FIG. 1; see also [0017] "***a computer kiosk*** *12 which is located in a retail store 14... contains demonstration versions of software and, if desired, full version of the software*").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas Jr.'s approach to include a computer kiosk to allow the user to select and recording the selection of software for download. One would have been motivated to modify because the computer kiosk provides an easy and convenient way to select and download software.

12. Claims 25, 33, 40, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (USPN 7,051,211).

As per claim 25:

Matyas Jr. does not explicitly teach:

wherein interrogating the hardware unit to obtain information comprising preexisting software comprises executing a Desktop Management Interface.

However, official notice is taken that using Desktop Management Interface is well known to the art at the time the invention was made. One would have been motivated to use Desktop Management Interface to provide information about the BIOS and the computer system to the user in a standardized way.

As per claims 33, 40, and 51:

Matyas Jr. does not explicitly teach:

wherein the software is data comprising music, images, and video.

However, official notice is taken that downloading music, image, and video are well known to the art at the time the invention was made. Software comprises music, image, video, game, etc. One would have been motivated to modify Matyas Jr.'s approach to allow downloading music, image, and video to the client computer in order to fulfill the client's needs and desires.

13. Claims 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (USPN 7,051,211), in view of Kato et al. (USPN 6,470,496).

As per claims 31 and 32:

Matyas does not explicitly teach:

wherein the download transaction status comprises a transaction hold status.

However, Kato teaches:

wherein the download transaction status comprises a transaction hold status (see at least col. 18:27-41 "*The* ***status holding unit 158 holds a status value*** *that shows one out of:* ***status 1 from the start of downloading the new control program until the complete*** *transfer of the new download program to the control program storing unit 152...*").

Therefore, it would have been obvious to one having an ordinary skill in the art at the time the invention was made to modify Matyas Jr.'s approach to include transaction hold status taught by Kato. One would have been motivated to modify because it provides a status value that shows the start of downloading until the complete transfer of the download.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Phillip H. Nguyen whose telephone number is (571) 270-1070. The examiner can normally be reached on Monday - Thursday 10:00 AM - 3:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Y. Zhen can be reached on (571) 272-3708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

4/25/2008

/Wei Zhen/
Supervisory Patent Examiner, Art Unit 2191